

Detecting separable states via semidefinite programs

Federico M. Spedalieri^{1,*}

¹*Department of Electrical Engineering, University of California, Los Angeles, Los Angeles, California 90095*

(Dated: February 1, 2008)

We introduce a new technique to detect separable states using semidefinite programs. This approach provides a sufficient condition for separability of a state that is based on the existence of a certain local linear map applied to a known separable state. When a state is shown to be separable, a proof of this fact is provided in the form of an explicit convex decomposition of the state in terms of product states. All states in the interior of the set of separable states can be detected in this way, except maybe for a set of measure zero. Even though this technique is more suited for a numerical approach, a new analytical criterion for separability can also be derived.

I. INTRODUCTION

Entanglement is one of the most important resources for quantum information processing. It allows us to perform such tasks as teleportation, secure quantum key distribution, superdense coding and quantum computation to name a few [1]. Because of its central role a great deal of effort has been put into its characterization in the past few years.

One of the most important questions, and also one very difficult to answer in general, is whether a given mixed state is entangled or separable. The decision problem associated with this characterization has been shown to be NP-hard [2], so a simple practical procedure to answer this question is not likely to exist. To tackle the problem, many incomplete criteria have been developed in the form of either necessary or sufficient conditions for separability. Several of these criteria are based on relatively easy to verify properties that separable states must satisfy. If a given state fails such a test, it must be entangled. However, if the state passes the test, the result is inconclusive. This type of criteria includes the positive partial transpose (PPT) criterion [3, 4] and its extensions [5, 6], the reduction criterion [7] and the range criterion [8] among others.

In this paper we introduce a new criterion for separability that works in a complementary way. If a given state passes a certain test, the state must be separable. Furthermore, a proof of this fact is given as an explicit convex decomposition of the state in terms of product states. The criterion is based on the fact that separable states preserve their separability property when a local map with certain properties acts on them. This local map need not be a physically implementable map, or even a positive map. The key point is that the search for such map can be implemented as a semidefinite program (SDP), which is a class of convex optimization problems for which efficient algorithms are known [9]. Semidefinite programs have found widespread application in quantum information [5, 10, 11, 12]. Even though this new cri-

terion is formulated in a way that is best suited for a numerical approach, it can also be used to derive a new analytical condition for separability.

The paper is organized as follows. In Section I we present the basic idea of our approach by looking at the action of local maps on separable states. In Section II we introduce the concept of base states and discuss the properties they must have. Section III introduces an improved approach that can detect more separable states. Section IV deals with the problem of characterizing the set of states that are detected by this procedure. Section V shows how to extract a new analytical criterion for separability and serves as an illustration of the technique. Finally, the conclusions are presented in Section VI.

II. LOCAL MAPS ON SEPARABLE STATES

Let ρ_0 be a separable state on $\mathcal{H}_A \otimes \mathcal{H}_B$, where for now we will consider that $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$. Then, by definition, we know that ρ_0 can be written as a convex combination of product states, namely

$$\rho_0 = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \quad (1)$$

with $0 \leq p_i \leq 1$, $\sum_i p_i = 1$ and $\rho_A^{(i)}$ and $\rho_B^{(i)}$ are density matrices in \mathcal{H}_A and \mathcal{H}_B respectively. Suppose that we have a linear map Λ on density matrices over \mathcal{H}_B , that satisfies $\Lambda(\rho_B^{(i)}) \geq 0$ for all i (where the inequality means the matrix is positive semidefinite (PSD)). Then, if we apply the map $\mathcal{I} \otimes \Lambda$ to ρ_0 , the resulting state ρ is, up to some normalization constant, also a separable state, since

$$\rho = \mathcal{I} \otimes \Lambda(\rho_0) = \sum_i p_i \rho_A^{(i)} \otimes \Lambda(\rho_B^{(i)}), \quad (2)$$

gives a decomposition of ρ as a convex combination of product states. Note that Λ need not be a positive map, since it is only required to be positive over a (typically) finite set of density matrices over \mathcal{H}_B . Furthermore, since Λ may not even be normalized (in the sense that $\text{Tr}[\Lambda(\rho_B^{(i)})]$ may not be equal to 1), after the appropriate

*Electronic address: federico@ee.ucla.edu

normalization the probabilities p_i in the decomposition of ρ may be different from those in the decomposition of ρ_0 .

Our approach to identifying separable states will be based precisely on this simple observation. Basically, given a state σ , if we find a map Λ satisfying the above mentioned criterion, and such that $\sigma = \mathcal{I} \otimes \Lambda(\rho_0)$, we can assure that σ is a separable state. Furthermore, we will be able to provide a proof of this fact in the form of an explicit decomposition of σ as a convex combination of product states. We will see that the search for this map corresponds to solving a linear system and checking for the appropriate positivity requirements afterwards. Then we will show that we can slightly modify our basic observation (2) to enlarge the set of maps that would allow us to detect separable states, and we will show that this new search can be cast as a semidefinite program.

It is clear that for this approach to be useful, we need to start with a separable state ρ_0 for which we know an explicit decomposition of the form (1). We will refer to such a state as a *base state*, since it is used as a “base” from which to reach other separable states. The usefulness of this technique depends on how the state ρ_0 is chosen, and we will start by discussing what properties it must have.

III. BASE STATES

Given a state σ the question of whether it satisfies $\sigma = \mathcal{I} \otimes \Lambda(\rho_0)$ for some map Λ can be answered by solving a linear system of equations. Both σ and ρ_0 can be decomposed with respect to a basis for density matrices over $\mathcal{H}_A \otimes \mathcal{H}_B$ as

$$\rho_0 = \sum_{m,n,r,s=1}^d R_{mnrs} |m\rangle\langle n| \otimes |r\rangle\langle s|, \quad (3)$$

and

$$\sigma = \sum_{m,n,r,s=1}^d S_{mnrs} |m\rangle\langle n| \otimes |r\rangle\langle s|. \quad (4)$$

We can also define a basis on the linear space of maps over operators in \mathcal{H}_B given by the set of maps $\{\Lambda_{ijkl}\}_{i,j,k,l=1}^d$ that satisfy

$$\Lambda_{ijkl}(|r\rangle\langle s|) = |k\rangle\langle l| \delta_{ir} \delta_{js}. \quad (5)$$

The most general linear map can then be written as $\Lambda = \sum_{i,j,k,l=1}^d x_{ijkl} \Lambda_{ijkl}$, for some arbitrary coefficients x_{ijkl} . Then the equation $\sigma = \mathcal{I} \otimes \Lambda(\rho_0)$ reduces to a system of linear equations given by

$$S_{mnkl} = \sum_{r,s=1}^d R_{mnrs} x_{klrs}. \quad (6)$$

This is a system of d^4 equations with d^4 unknowns. It will always have a solution, but we also need to impose on

this solution the positivity conditions $\Lambda(\rho_B^{(i)}) \geq 0, \forall i$. If the linear system (6) has a unique solution, we can check these conditions by computing eigenvalues. If the system is undetermined we can solve for some of the coefficients x_{ijkl} and write $\Lambda = \Lambda_0 + \sum_J \Lambda_J$, where Λ_0 is the fixed part of the solution and the sum groups the remaining terms. Thus the problem reduces to checking whether the map Λ is positive over the set $\{\rho_B^{(i)}\}$. This can be written as a linear matrix inequality (LMI), and so we can cast our problem in the form of the semidefinite program (SDP)

$$\begin{aligned} & \min && 0 \\ & \text{subject to} && \bigoplus_i \Lambda_0(\rho_B^{(i)}) + \sum_J x_J \bigoplus_i \Lambda_J(\rho_B^{(i)}) \geq 0. \end{aligned} \quad (7)$$

The size of the SDP will be determined by the dimension d and the number of terms in the decomposition (1) of ρ_0 . Caratheodory's theorem [13] assures that any separable state can be decomposed as a convex combination of at most $d^4 + 1$ product states, so the size of the SDP remains polynomial in d . We will see later that we would have ample freedom to choose the base state ρ_0 , and so we can keep the size of the SDP under control.

The uniqueness of the solution of the system (6) depends on whether the matrix of the system is invertible or not. From (6) we can see that this matrix will depend only on the components R_{mnrs} , and hence it is completely determined by the base state ρ_0 . From this point of view it is a bit cumbersome to determine whether a given base state makes the system (6) invertible or not. Fortunately there is an alternative way of looking at this problem that connects with previous work and provides us with a nicer and more practical characterization of base states.

First, let us note that for a fixed base state ρ_0 we can regard the expression $\mathcal{I} \otimes \Lambda(\rho_0)$ as a function that assigns to every map Λ the operator $\mathcal{I} \otimes \Lambda(\rho_0)$. Note that we refer to it as an operator and not a state, since we have imposed no conditions on Λ , which may not be positive. If we choose $\rho_0 = |\psi^+\rangle\langle\psi^+|$ (with $|\psi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |ii\rangle$ the maximally entangled state), then we know that the linear function $f(\Lambda) = \mathcal{I} \otimes \Lambda(|\psi^+\rangle\langle\psi^+|)$ has very important and useful properties. It defines an isomorphism between the set of completely positive (CP) maps, mapping states over \mathcal{H}_B to states over \mathcal{H}_A , and the set of states over $\mathcal{H}_A \otimes \mathcal{H}_B$. This is known as the *Jamiołkowski isomorphism* [14]. In [15] D'Ariano and Lo Presti studied whether other bipartite states besides the maximally entangled state will induce a one to one mapping between CP maps and states. They found that there are indeed such states and derived a very simple test to identify them: a state ρ_0 will induce such a mapping if the operator $\check{\rho}_0 = (E\rho_0)^{T_B} E$, is invertible, with $E = \sum_{ij} |ij\rangle\langle ji|$ the swap operator. They called such a state a *faithful* state. Furthermore, from this characterization it is easy to see that the set of faithful states is *dense* over the set of all states, and so we can have faithful states that are separable. However, we should

note that separable pure states cannot be faithful. In fact, if $\rho_0 = |x\rangle\langle x| \otimes |y\rangle\langle y|$ (where $|x\rangle = \sum_i x_i |i\rangle$ and $|y\rangle = \sum_i y_i |i\rangle$), then $\tilde{\rho}_0 = |y\rangle\langle x^*| \otimes |y^*\rangle\langle x|$, which is clearly not invertible.

If we use a faithful state as a base state, the function f is a one to one mapping between CP maps and positive semidefinite operators. In terms of the linear system (6) this means that the system must be invertible since the relationship between states and maps must be one to one. Similarly, if the system (6) is invertible the state ρ_0 must be faithful. It is clear then that if we use a faithful state as a base state, a larger set of separable states can be detected than if we use nonfaithful states.

IV. GEOMETRIC PICTURE AND IMPROVED ALGORITHM

There is a nice geometric picture of our technique to detect separable states. First let us note that the set of all states is the intersection of the cone of positive semidefinite matrices (known as the PSD cone) and the hyperplane defined by the normalization condition $\text{Tr}[\rho] = 1$. The normalization does not affect the separability property of a state, so in order to make our discussion simpler we will sometimes analyze and prove results in terms of the cone structure of a set of states. It will be straightforward to understand those results in terms of the actual set of states satisfying the normalization condition $\text{Tr}[\rho] = 1$.

Let us assume that we have a faithful base state ρ_0 that is separable and has a convex decomposition given by (1). The set of maps $K_B = \{\Lambda : \Lambda(\rho_B^{(i)}) \geq 0, \forall i\}$, is a *cone* (that is, a set closed under linear combinations with nonnegative coefficients). The linear map g given by $g(\Lambda) = \mathcal{I} \otimes \Lambda(\rho_0)$, maps K_B into another cone contained in the set of separable states (which is itself a cone). It is not difficult to see that this image cone has nonzero measure. First note that K_B contains the cone of CP maps which is in one to one correspondence with the PSD cone in $\mathcal{H}_A \otimes \mathcal{H}_B$ (the cone associated with bipartite density matrices) via the linear map f defined in the previous section. Both the cone of CP maps and the PSD cone are embedded in vector spaces of the same dimension d^4 , and since the PSD cone has nonzero measure, it follows that so do the CP cone and K_B . Since the map g is linear and one to one, it will send a nonzero measure set into a nonzero measure set.

We have seen that our approach reduces to solving a linear system and checking certain positivity properties of the solution. In particular if we use a faithful state as a base state, such linear system has a unique solution, so no semidefinite program is required. However, we can improve our technique by considering a slightly more general type of mapping. Instead of considering $g(\Lambda) = \mathcal{I} \otimes \Lambda(\rho_0)$ we can analyze the more general linear

map

$$\sigma = [\mathcal{I} \otimes \Lambda_B + \Lambda_A \otimes \mathcal{I}](\rho_0), \quad (8)$$

with $\Lambda_B \in K_B$ and $\Lambda_A \in K_A$, where $K_A = \{\Lambda_A : \Lambda_A(\rho_A^{(i)}) \geq 0, \forall i\}$. The maps of the form $\mathcal{I} \otimes \Lambda_B + \Lambda_A \otimes \mathcal{I}$ also form a cone K_{AB} that contains both K_A and K_B . If ρ_0 is a faithful separable state, the map (8) sends all elements of K_{AB} into the cone of separable states, and hence detects at least the same set of separable states than the map g alone. And finally, the search for a map in K_{AB} that satisfies (8) for some state σ is indeed a semidefinite program.

V. CHARACTERIZING THE SET OF DETECTED STATES

The image of the cone K_B under the map g determines the set of separable states that can be detected for a particular base state ρ_0 . We have seen that the best choice for ρ_0 is a faithful separable state, since in that case the mapping g is one to one and hence the image of K_B is as large as possible. This leads us to the obvious question of how big this cone is, or how much of the set of separable states can be detected in this way. So far we know that the set of detectable separable states (for a fixed faithful base state) is a cone of nonzero measure contained in the cone of separable states. We do not expect it to be the whole cone of separable states, since the separability problem is NP-hard and our characterization is polynomial. However we will show that we can detect in this way any state in the interior of the set of separable states S , except maybe for a set of measure zero.

One set of states that we can assure will be detected is the set of separable faithful states in the interior of S , which is a set whose complement (with respect to S°) has zero measure. Let $K^+(\rho_0) = \{\sigma : \sigma = \mathcal{I} \otimes \Lambda(\rho_0), \text{ with } \Lambda \text{ a positive map}\}$. This is also a cone and it is contained in the cone of states characterized by the SDP discussed in the previous section. Even though this is a smaller set of states, it is enough to prove all the properties we want to present. Note that it is clear that for any faithful state ρ_0 (actually any state), $\rho_0 \in K^+(\rho_0)$, since we can just take Λ to be the identity map. But this observation is not at all helpful since we need to know if ρ_0 is actually separable in order for this approach to be useful. Fortunately, for faithful states in S° we can prove a stronger result:

Theorem 1 *Let σ be a faithful state in S° . There is another faithful state $\rho_0 \in S^\circ$ such that $\sigma \in (K^+(\rho_0))^\circ$.*

Proof: Let $\sigma \in S^\circ$. Consider the linear map $h(\Lambda) = \mathcal{I} \otimes \Lambda(\sigma)$. By the continuity of this map, there is a neighborhood A of the identity map \mathcal{I} such that if $\Lambda \in A \Rightarrow h(\Lambda) \in S^\circ$. Furthermore, since the identity map is invertible, there is a neighborhood $B \subseteq A$ such that all maps in B are also invertible. Let inv be

the inverse function, that sends any invertible map to its inverse. Then it is clear that $\text{inv} = \text{inv}^{-1}$. This together with the fact that inv is a continuous function tells us that inv send open sets into open sets. Consider then the open set $B^{-1} = \text{inv}(B)$. Since $\mathcal{I} \in B$ and $\mathcal{I}^{-1} = \mathcal{I}$, then $\mathcal{I} \in B^{-1}$. On the other hand, the identity map is on the boundary of the set of positive maps since an arbitrarily small perturbation of this map can send a PSD operator into a non-PSD operator. Therefore the intersection of B^{-1} with the interior of the set of positive maps is a nonempty open set C . Now consider the open set $C^{-1} = \text{inv}(C)$. Clearly, $C^{-1} \subset A$ and every element Λ of C^{-1} is a map that satisfies (i) $\Lambda \in A$ and hence $h(\Lambda) \in S^\circ$, and (ii) Λ is invertible and Λ^{-1} is a positive map. Finally, consider the set $h(C^{-1}) \subset S^\circ$. This is a nonempty open subset of S° , and so it must contain a faithful state ρ_0 (different from σ since the identity map is not in C^{-1}), because faithful states are dense in the set of states. Then there is a map $\bar{\Lambda}^{-1}$ in C^{-1} such that $\rho_0 = \mathcal{I} \otimes \bar{\Lambda}^{-1}(\sigma)$. Therefore the map $\bar{\Lambda} \in C$ satisfies $\sigma = \mathcal{I} \otimes \bar{\Lambda}(\rho_0)$, with $\bar{\Lambda}$ positive. Since C is an open set contained in the interior of the set of positive maps, and the function $g(\Lambda) = \mathcal{I} \otimes \Lambda(\rho_0)$ is linear and one to one, σ must belong to $(K^+(\rho_0))^\circ$. \square

The preceding theorem tells us that any separable faithful state can be detected using a different separable faithful state as a base state. This comprises all of the set of separable states except for a set of measure zero (namely, the set of nonfaithful states and the states in the boundary of S that we have left out of this discussion.) We will see that some nonfaithful states are also detected by this procedure. To understand this we need the following lemma:

Lemma 1 *Let ρ_0 be a faithful state in S . The state $\sigma = \mathcal{I} \otimes \bar{\Lambda}(\rho_0)$ with $\bar{\Lambda}$ a positive map is also separable and faithful if and only if the map $\bar{\Lambda}$ is invertible.*

Proof: Consider the function $f(\Lambda) = \mathcal{I} \otimes \Lambda(\sigma)$. The state σ is faithful if and only if this function is one to one. We can rewrite f as $f(\Lambda) = \mathcal{I} \otimes (\Lambda \circ \bar{\Lambda})(\rho_0)$. If $\bar{\Lambda}$ is invertible then f is one to one, since $f(\Lambda_1) = f(\Lambda_2)$ implies that $\Lambda_1 \circ \bar{\Lambda} = \Lambda_2 \circ \bar{\Lambda}$ because ρ_0 is faithful, and so $\Lambda_1 = \Lambda_2$ because $\bar{\Lambda}$ is invertible. To prove the converse, assume that σ is faithful and that $\bar{\Lambda}$ is not invertible, so that $\text{Ker}(\bar{\Lambda}) \neq \emptyset$. We can choose two maps Λ_1 and Λ_2 , $\Lambda_1 \neq \Lambda_2$ such that they are distinct only over $\text{Ker}(\bar{\Lambda})$. Then we have that $\Lambda_1 \circ \bar{\Lambda} = \Lambda_2 \circ \bar{\Lambda}$. Now we can write

$$\begin{aligned} f(\Lambda_1) &= \mathcal{I} \otimes \Lambda_1(\sigma) \\ &= \mathcal{I} \otimes (\Lambda_1 \circ \bar{\Lambda})(\rho_0) \\ &= \mathcal{I} \otimes (\Lambda_2 \circ \bar{\Lambda})(\rho_0) \\ &= \mathcal{I} \otimes \Lambda_2(\sigma) = f(\Lambda_2), \end{aligned} \quad (9)$$

which is a contradiction to the fact that f is one to one since σ is faithful. Thus, $\bar{\Lambda}$ must be invertible. \square

This result shows that there are nonfaithful states that are detected, since we can easily construct a noninvertible positive map Λ and hence the state $\mathcal{I} \otimes \Lambda(\rho_0)$ is not

faithful and belongs to $K^+(\rho_0)$ for ρ_0 faithful. However this is not enough to say that all nonfaithful states can be detected. Whether there are nonfaithful states that cannot be detected in this way is an interesting and open problem at this point.

Another interesting result is given by the following lemma:

Lemma 2 *Let ρ_1 and ρ_2 be faithful states such that $\rho_2 \in K^+(\rho_1)$. Then $K^+(\rho_2) \subseteq K^+(\rho_1)$.*

Proof: Let $\sigma \in K^+(\rho_2)$. Then $\sigma = \mathcal{I} \otimes \Lambda(\rho_2)$ for some positive map Λ . Since $\rho_2 \in K^+(\rho_1)$, there is a positive map Λ' such that $\rho_2 = \mathcal{I} \otimes \Lambda'(\rho_1)$. Combining the two equations we have that $\sigma = \mathcal{I} \otimes (\Lambda \circ \Lambda')(\rho_1)$. Since the composition of two positive maps is also a positive map, then $\sigma \in K^+(\rho_1)$, and hence $K^+(\rho_2) \subseteq K^+(\rho_1)$. \square

An interesting picture of the set of separable states begins to emerge. By combining Theorem 1 and Lemma 2 we can conclude that for any faithful state ρ_2 in S° we can always find another faithful state ρ_1 also in S° such that $K^+(\rho_2) \subseteq K^+(\rho_1)$. We could then construct a sequence of cones $K^+(\rho_n)$ such that $K^+(\rho_n) \subseteq K^+(\rho_{n+1})$. We do not expect this sequence of cones to contain all possible detectable states asymptotically, but rather to grow to some sort of maximal cone that will define a domain inside the set of separable states. Since this domain cannot be the whole set S , we expect that there will be other domains constructed in the same way, using faithful base states that are not contained in any of the cones $K^+(\rho_n)$. These domains must cover the whole interior of S except maybe for a set of measure zero, comprised only of nonfaithful states.

To summarize, the procedure for detecting separable states could be applied as follows. Given a state σ we want to check for separability, we first generate a random separable state by randomly generating the terms in the decomposition

$$\rho_0 = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \quad (10)$$

i.e., randomly choosing the number of terms in the decomposition, the probabilities p_i and the local density matrices $\rho_A^{(i)}$ and $\rho_B^{(i)}$. We can simplify this step by noting any separable state can be written as a convex combination of pure product states with at most $d^4 + 1$ terms. Then we check whether this random separable state is faithful or not by checking if the operator $\tilde{\rho}_0 = (E\rho_0)^{T_B}E$ is invertible (with $E = \sum_{ij} |ij\rangle\langle ji|$ the swap operator.) Since the set of nonfaithful states has zero measure, our random state will be most likely faithful. Then, we can just solve the enhanced SDP discussed in Section IV, and if a feasible solution exists, we have proven that σ is separable, and can furthermore construct an explicit convex decomposition of it in terms of product states. If the SDP turns out to be unfeasible, it means that σ could be entangled, or that we need a different faithful base state. We could then select a new faithful base state and proceed as before.

Since each faithful state can help us to identify many separable states, it could be useful to save them for use with other states. We can then build up a table of faithful separable states for each dimensionality, so we can bypass the random generation step in the future. Furthermore, this table can be optimized by discarding any state ρ_2 that belongs to $K^+(\rho_1)$ for some ρ_1 also in the table, since according to Lemma 2 it will not detect any new states. Another interesting and open problem is whether we can make this table finite and still detect most of the states in S° except maybe for a set of arbitrarily small (but not zero) measure. That finite number of base states will probably depend on the dimensions of the problem (and the measure of the undetected set), but this approach might turn out to be a useful tool for low dimensional problems.

A. Extension to $d_A \neq d_B$

Our approach to detect separable states can be extended to the case in which the dimensions of the spaces \mathcal{H}_A and \mathcal{H}_B are not equal, with a few minor modifications. To see how this works we first need to state the Jamiolkowski isomorphism in its more general form. Let \mathcal{H}_A and \mathcal{H}_B be two spaces of dimensions d_A and d_B respectively. We will denote by $\mathcal{B}(\mathcal{H})$ the set of bounded, PSD operators over the Hilbert space \mathcal{H} . Let $\mathcal{L}(\mathcal{B}(\mathcal{H}_A), \mathcal{B}(\mathcal{H}_B))$ be the set of CP maps from $\mathcal{B}(\mathcal{H}_A)$ to $\mathcal{B}(\mathcal{H}_B)$. Then the function $F : \mathcal{L}(\mathcal{B}(\mathcal{H}_A), \mathcal{B}(\mathcal{H}_B)) \rightarrow \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, defined by

$$F(\Lambda) = \mathcal{I} \otimes \Lambda(|\psi^+\rangle_{AA} \langle\psi^+|), \quad (11)$$

where $|\psi^+\rangle_{AA}$ is the maximally entangled state in $\mathcal{H}_A \otimes \mathcal{H}_A$, is an *isomorphism* between CP maps in $\mathcal{L}(\mathcal{B}(\mathcal{H}_A), \mathcal{B}(\mathcal{H}_B))$ and PSD operators in $\mathcal{H}_A \otimes \mathcal{H}_B$.

Now let us define another function $\tilde{F} : \mathcal{L}(\mathcal{B}(\mathcal{H}_A), \mathcal{B}(\mathcal{H}_B)) \rightarrow \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, given by

$$\tilde{F}(\Lambda) = \mathcal{I} \otimes \Lambda(\rho_0), \quad (12)$$

with ρ_0 a faithful separable state in $\mathcal{H}_A \otimes \mathcal{H}_A$. It is clear that $\tilde{F}(\Lambda)$ is also a separable state in $\mathcal{H}_A \otimes \mathcal{H}_B$ provided that Λ satisfies the same positivity conditions we required in the case $d_A = d_B$. By the same isomorphism, applied to states in $\mathcal{H}_A \otimes \mathcal{H}_A$, we know that there must be a CP map $\Lambda_0 : \mathcal{B}(\mathcal{H}_A) \rightarrow \mathcal{B}(\mathcal{H}_A)$ such that

$$\rho_0 = \mathcal{I} \otimes \Lambda_0(|\psi^+\rangle_{AA} \langle\psi^+|). \quad (13)$$

Furthermore, following the same reasoning as in the proof of Lemma 1, we conclude that the map Λ_0 must be invertible (note that this inverse will not be in general a CP map.) And using the same argument once again, it is not difficult to show that the function \tilde{F} must be one to one. By the same arguments of the case $d_A = d_B$, we can then conclude that the set of detected states is also of nonzero measure when $d_A \neq d_B$. The only difference

between these two cases is that in the latter the faithful states must be chosen from a space different than the one in which the states to be detected live.

B. Multipartite states

It is interesting to see what happens with this approach when we apply it to multipartite states. Even though the basic property that allows us to connect two separable states is still valid, the results are not as useful because the set of detected states has zero measure even for faithful states. Let us briefly show the reason in the tripartite case. Let ρ_0 be a separable state in $\mathcal{H}_A \otimes \mathcal{H}_A \otimes \mathcal{H}_A$, with $\dim \mathcal{H}_A = d$. Clearly, any state of the form $\sigma = [\mathcal{I} \otimes \mathcal{I} \otimes \Lambda](\rho_0)$, is separable if Λ satisfies the required positivity constraints. The cone of separable tripartite states is embedded in a vector space of dimension d^8 . But the set of linear maps Λ is embedded in a space of dimension d^4 , so even if ρ_0 is a faithful state, the mapping of Λ to σ produces a set of dimension d^4 embedded in a space of dimension d^8 . Hence, the image of this mapping (which is the set of detected states) has zero measure with respect to the cone of tripartite separable states, and this makes this approach not useful in practice. One solution to this problem will be to consider transformations of the form $\sigma = [\mathcal{I} \otimes \Lambda_A \otimes \Lambda_B](\rho_0)$ but then checking for the existence of the maps Λ_A and Λ_B becomes a nonlinear problem that cannot be solved using SDP.

VI. ANALYTICAL CRITERION

This technique can also help us to derive some analytical results about separability. By choosing a particular base state, and using some results on the characterization of positive maps [5], we can obtain a sufficient condition for separability in terms of the eigenvalues of an associated state.

Consider the following family of states

$$\rho(\lambda) = (1 - \lambda)I_{AB} + \lambda|\psi^+\rangle\langle\psi^+|, \quad (14)$$

where $0 \leq \lambda \leq 1$, I_{AB} is the maximally mixed state in $\mathcal{H}_A \otimes \mathcal{H}_B$ (i.e., the identity matrix times $\frac{1}{d^2}$, since we are considering $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$), and $|\psi^+\rangle = \frac{1}{\sqrt{d}} \sum_i |ii\rangle_{AB}$ is the maximally entangled state. These states are referred to as the *isotropic states* (since they are invariant under $U \otimes U^*$ transformations) and are known to be separable for $0 \leq \lambda \leq \frac{1}{d+1}$, and entangled otherwise. We will choose $\rho_0 = \rho(\frac{1}{d+1})$. This state is in the boundary of S and it is not difficult to check that it is faithful.

Let σ be a state that satisfies

$$\sigma = \mathcal{I} \otimes \Lambda(\rho_0), \quad (15)$$

for some positive map Λ . This is equivalent to

$$\sigma = \mathcal{I} \otimes \Lambda\left(\frac{d}{d+1}I_{AB}\right) + \mathcal{I} \otimes \Lambda\left(\frac{1}{d+1}|\psi^+\rangle\langle\psi^+|\right). \quad (16)$$

Let us impose a restriction on Λ and require $\Lambda(I_B) = I_B$. We will see later that this restriction can be eliminated, but for now it simplifies the reasoning. Then we can rewrite (16) as

$$\sigma = \frac{d}{d+1}I_{AB} + \frac{1}{d+1}\mathcal{I} \otimes \Lambda(|\psi^+\rangle\langle\psi^+|). \quad (17)$$

The restriction on Λ means that, for consistency, we must have $\text{Tr}_A[\sigma] = I_B$. Again, this restriction can be lifted and we will see that later on. We now write

$$\sigma - \frac{d}{d+1}I_{AB} = \mathcal{I} \otimes \tilde{\Lambda}(|\psi^+\rangle\langle\psi^+|), \quad (18)$$

where we have rescaled the positive map, so $\tilde{\Lambda} = \frac{1}{d+1}\Lambda$.

From the Jamiołkowski isomorphism we also know that any operator Z of the form

$$Z = \mathcal{I} \otimes \tilde{\Lambda}(|\psi^+\rangle\langle\psi^+|), \quad (19)$$

with $\tilde{\Lambda}$ a positive map, must be positive over the set of separable states. This is equivalent to the associated bihermitian form

$$\begin{aligned} E_Z &= \langle xy|Z|xy\rangle \\ &= \sum_{ijkl} x_i^* y_j^* x_k y_l \langle ij|Z|kl\rangle, \end{aligned} \quad (20)$$

being nonnegative. In [5] a sequence of tests was introduced (each test implementable as a SDP) that could prove the positivity of the form E_Z , and hence the existence of a positive map satisfying (19).

Consider our state σ that satisfies $\text{Tr}_A[\sigma] = I_B$ and let us assume that we can prove that the bihermitian form associated with the operator $(\sigma - \frac{d}{d+1}I_{AB})$ is positive, using the techniques from [5]. Then, by the Jamiołkowski isomorphism, the map $\tilde{\Lambda}$ that satisfies

$$\sigma - \frac{d}{d+1}I_{AB} = \mathcal{I} \otimes \tilde{\Lambda}(|\psi^+\rangle\langle\psi^+|), \quad (21)$$

is positive. By tracing over A on both sides it is not difficult to show that $\tilde{\Lambda}(I_B) = \frac{1}{d+1}I_B$, so we can write

$$\sigma - \frac{d}{d+1}I_{AB} = \frac{1}{d+1}\mathcal{I} \otimes \Lambda(|\psi^+\rangle\langle\psi^+|), \quad (22)$$

where now Λ satisfies $\Lambda(I_B) = I_B$. Since $I_{AB} = I_A \otimes I_B$ we can write $I_{AB} = \mathcal{I} \otimes \Lambda(I_{AB})$ and then we have that

$$\begin{aligned} \sigma &= \mathcal{I} \otimes \Lambda\left(\frac{d}{d+1}I_{AB}\right) + \mathcal{I} \otimes \Lambda\left(\frac{1}{d+1}|\psi^+\rangle\langle\psi^+|\right) \\ &= \mathcal{I} \otimes \Lambda(\rho_0), \end{aligned} \quad (23)$$

which shows that σ is separable.

Assume now that we have a state σ that satisfies $\text{Tr}_A[\sigma] = \sigma_B > 0$, so that σ_B is invertible. Note that any state in the interior of S will have this property. We can construct the state

$$\tilde{\sigma} = \frac{1}{d}(\mathbf{1}_A \otimes \sigma_B^{-\frac{1}{2}})\sigma(\mathbf{1}_A \otimes \sigma_B^{-\frac{1}{2}}), \quad (24)$$

that satisfies the condition $\text{Tr}_A[\tilde{\sigma}] = I_B$ (with $\mathbf{1}_A$ the identity matrix in d dimensions). It is clear that if $\tilde{\sigma}$ is separable, so is σ .

According to our discussion above, we can prove separability of $\tilde{\sigma}$ by proving positivity of the bihermitian form associated with the operator $\tilde{\sigma} - \frac{d}{d+1}I_{AB}$. Clearly, a sufficient (but not necessary) condition for this to be true is the that the operator $\tilde{\sigma} - \frac{d}{d+1}I_{AB}$ itself be positive semidefinite. If λ_i are the eigenvalues of $\tilde{\sigma}$, this is equivalent to requiring that $\min_i \lambda_i \geq \frac{1}{d(d+1)}$. We then have the following corollary:

Corollary 1 *Let σ be a state in $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$, that satisfies $\text{Tr}_A[\sigma] = \sigma_B > 0$. Let $\tilde{\sigma} = \frac{1}{d}(\mathbf{1}_A \otimes \sigma_B^{-\frac{1}{2}})\sigma(\mathbf{1}_A \otimes \sigma_B^{-\frac{1}{2}})$, with eigenvalues λ_i . If*

$$\min_i \lambda_i \geq \frac{1}{d(d+1)}, \quad (25)$$

then σ is separable.

Furthermore, for any state σ shown to be separable as a consequence of Corollary 1, we can provide an explicit convex decomposition in terms of product states. From the Jamiołkowski isomorphism we can also extract an explicit expression of the map Λ in terms of the hermitian operator Z that satisfies $Z = \mathcal{I} \otimes \Lambda(|\psi^+\rangle\langle\psi^+|)$. In our case, given an orthonormal product basis $\{|ij\rangle_{AB}\}$, we can write

$$\Lambda(\rho) = \sum_{ijkl} \langle ij|(\tilde{\sigma} - \frac{d}{d+1}I_{AB})|kl\rangle \langle i|\rho|k\rangle \langle j|l\rangle, \quad (26)$$

where $\tilde{\sigma}$ is given by (24). Now we just need a decomposition of our base state

$$\rho_0 = \frac{d}{d+1}I_{AB} + \frac{1}{d+1}|\psi^+\rangle\langle\psi^+|. \quad (27)$$

In [16] one such decomposition of ρ_0 was given and we will follow that construction. First, let us define a vector $\mathbf{z} = (z_1, \dots, z_d)$, whose components z_j take on the values ± 1 and $\pm i$. To each vector \mathbf{z} we associate a pure state

$$|\Phi_{\mathbf{z}}\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d z_j |j\rangle, \quad (28)$$

with $\{|j\rangle\}$ the canonical basis. There are 4^d such vectors, and hence 4^d states $|\Phi_{\mathbf{z}}\rangle$, although only 4^{d-1} are distinct in that they differ by more than a global phase. Now we define a product state in $\mathcal{H}_A \otimes \mathcal{H}_B$ given by

$$\rho_{\mathbf{z}} = |\Phi_{\mathbf{z}}\rangle\langle\Phi_{\mathbf{z}}| \otimes |\Phi_{\mathbf{z}^*}\rangle\langle\Phi_{\mathbf{z}^*}|. \quad (29)$$

The ensemble consisting of all 4^d of these states with the same probability gives the density operator

$$\frac{1}{4^d} \sum_{\mathbf{z}} \rho_{\mathbf{z}} = \frac{1}{4^d d^2} \sum_{jklm} \left(\sum_{\mathbf{z}} z_j z_k^* z_l^* z_m \right) |j\rangle\langle k| \otimes |l\rangle\langle m|. \quad (30)$$

Since

$$\sum_{\mathbf{z}} z_j z_k^* z_l^* z_m = 4^d (\delta_{jk} \delta_{lm} + \delta_{jl} \delta_{km} - \delta_{jk} \delta_{lm} \delta_{jl}), \quad (31)$$

it follows that

$$\frac{1}{4^d} \sum_{\mathbf{z}} \rho_{\mathbf{z}} = I_{AB} + \frac{1}{d} |\psi^+\rangle\langle\psi^+| - \frac{1}{d^2} \sum_{j=1}^d |j\rangle\langle j| \otimes |j\rangle\langle j|. \quad (32)$$

Multiplying by $\frac{d}{d+1}$ and rearranging terms we get

$$\rho_0 = \frac{d}{d+1} \frac{1}{4^d} \sum_{\mathbf{z}} \rho_{\mathbf{z}} + \frac{1}{(d+1)d} \sum_{j=1}^d |j\rangle\langle j| \otimes |j\rangle\langle j|, \quad (33)$$

and hence we have

$$\begin{aligned} \sigma &= \frac{d^2}{d+1} \frac{1}{4^d} \sum_{\mathbf{z}} |\Phi_{\mathbf{z}}\rangle\langle\Phi_{\mathbf{z}}| \otimes \sigma_B^{\frac{1}{2}} \Lambda(|\Phi_{\mathbf{z}^*}\rangle\langle\Phi_{\mathbf{z}^*}|) \sigma_B^{\frac{1}{2}} + \\ &+ \frac{1}{(d+1)} \sum_{j=1}^d |j\rangle\langle j| \otimes \sigma_B^{\frac{1}{2}} \Lambda(|j\rangle\langle j|) \sigma_B^{\frac{1}{2}}, \end{aligned} \quad (34)$$

where $\sigma_B = \text{Tr}_A[\sigma]$ and Λ is given by (26). Since the map Λ is positive, Eq. (34) gives an explicit convex decomposition of σ in terms of product states, certifying its separability.

It is interesting to compare this corollary to the well-known result of Gurvits and Barnum [17] that characterizes the biggest ball of separable states centered on the maximally mixed state. Their result says that if $\|\sigma - I_{AB}\|_2^2 \leq \frac{1}{d^2(d^2-1)}$, then the state σ is separable. Now consider a state that satisfies $\text{Tr}_A[\sigma(\epsilon)] = I_B$ in the basis in which it is diagonal, and that

$$\sigma(\epsilon) = \text{diag}(\epsilon + \frac{1}{d(d+1)}, \lambda, \dots, \lambda), \quad (35)$$

where $\lambda = \frac{1}{d(d+1)} + \delta$ and both ϵ and δ are positive. By normalization we must have $\frac{d^2}{d(d+1)} + \epsilon + (d^2-1)\delta = 1$, and hence

$$\delta = (1 - \epsilon - \frac{d}{d+1}) \frac{1}{d^2-1}. \quad (36)$$

Since we need $\delta \geq 0$, we need $\epsilon \leq 1 - \frac{d}{d+1}$. If these conditions are satisfied, the state $\sigma(\epsilon)$ is separable. To see what the Gurvits-Barnum criterion says about such a state, we define the function

$$f(d, \epsilon) = \|\sigma(\epsilon) - I_{AB}\|_2^2 - \frac{1}{d^2(d^2-1)}. \quad (37)$$

If $f(d, \epsilon) > 0$ for $0 < \epsilon \leq 1 - \frac{d}{d+1}$, then the state $\sigma(\epsilon)$ is not shown as separable by the Gurvits-Barnum criterion, but it is by ours. It is easy to check that

$$f(d, 1 - \frac{d}{d+1}) = \frac{d-2}{d^3-d} > 0, \quad \forall d \geq 3. \quad (38)$$

Since $f(d, \epsilon)$ is a continuous function of ϵ , this shows that for $d \geq 3$, there is always a range of values of ϵ for which the state $\sigma(\epsilon)$ is shown to be separable by our technique but not by the Gurvits-Barnum criterion.

VII. CONCLUSIONS

In this paper we have introduced a new technique to detect separable states. The idea is to show that two states, the first of which is known to be separable and has certain properties, are connected by a local map that preserves separability. This local map is required to be positive on a set of local states determined by the convex decomposition of the first state in terms of product states. If a map with the required properties is found connecting the two states, the second state is proven to be separable. The key point is that searching for this connecting map reduces to a semidefinite program (SDP) which can be implemented efficiently. Furthermore, if the second state is proven to be separable, the solution of the SDP provides the required map and an explicit proof of separability of the second state can be constructed in the form of a convex decomposition in terms of product states.

It is important to note that the local map in question needs not be positive over all states. This is an advantage, since characterizing the set of positive maps is an NP-hard problem, while the wider set of maps we are interested in (which includes the set of positive maps) is easier to characterize and allows us to reduce the problem to a SDP. However, restricting ourselves to the set of positive maps makes it easier to prove and understand some properties of this technique. In particular, coupled with some previous work aimed at characterizing positive maps via an infinite hierarchy of conditions [5], it allowed us to extract a new criterion for separability based on the spectral properties of an associated state.

We have shown that all states in the interior of the set of separable states can be detected by this technique, except maybe for a set of measure zero. Our approach proceeds by choosing a random separable state (with a certain property known as *faithfulness* [15]) that we call *base states*, and implementing a SDP to check whether a given state is separable or not. The set of states detected using a particular base state is a convex subset of the set of separable states. By choosing different base states we are able to detect more and more separable states. We could keep a table of these states for future use much in the same way we keep the information about entanglement witnesses. Even though an infinite number of these states are needed to characterize all separable states, it may well be the case that a finite number will be enough

to characterize almost the whole set, except maybe for a set of very small (but not zero) measure. This is still an open question. Also open for further research is the structure of the set of separable states that cannot be detected using this technique. This structure seems to be related to the structure of the set of non invertible maps.

Finally, it is worth stressing that, as many other separability criteria, our technique is not complete, and should be complemented with other ways of analyzing entanglement and separability. One feature that should be pointed out is that our criteria either proves separability of the state (and provides a certificate of it in the form of an explicit decomposition) or fails. Other criteria usually show that the state is *entangled* or fail. These criteria generate an approximate characterization of the set of separable states from the outside. Our approach works *from the inside*. In this respect it is similar to the algo-

rithm presented in [18], that generates a sequence of convex sets included in the set of separable states for which membership can be easily checked. These two types of criteria (inside and outside characterizations) should be used together to increase the chance of correctly identifying the entanglement properties of a given state.

VIII. ACKNOWLEDGEMENTS

I would like to thank Vwani Roychowdhury for his support and suggestions, and Pablo Parrilo for many useful discussions. This work was supported by the MARCO/FCRP program, and the Western Institute of Nanoelectronics, a Nanoelectronics Research Initiative.

-
- [1] M. N. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
 - [2] L. Gurvits, in *STOC '03: Proceedings of the thirty-fifth annual ACM symposium on Theory of computing* (ACM Press, New York, NY, USA, 2003), pp. 10–19.
 - [3] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
 - [4] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
 - [5] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
 - [6] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).
 - [7] N. J. Cerf, C. Adami, and R. M. Gingrich, Phys. Rev. A **60**, 898 (1999).
 - [8] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
 - [9] L. Vandenberghe and S. Boyd, SIAM Review **38**, 49 (1996).
 - [10] E. M. Rains, quant-ph/0008047 (unpublished).
 - [11] F. G. S. L. Brandao and R. O. Vianna, Physical Review A **70**, 062309 (2004).
 - [12] A. S. Fletcher, P. W. Shor, and M. Z. Win, quant-ph/0606035 (unpublished).
 - [13] R. T. Rockafellar, *Convex Analysis* (Princeton University Press, Princeton, NJ, 1970).
 - [14] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).
 - [15] G. M. D'Ariano and P. Lo Presti, Phys. Rev. Lett. **91**, 047902 (2003).
 - [16] P. Rungta, Ph.D. thesis, University of New Mexico, 2002.
 - [17] L. Gurvits and H. Barnum, Phys. Rev. A **66**, 062311 (2002).
 - [18] F. Hulpke and D. Bruss, J. Phys. A:Math. Gen. **38**, 5573 (2005).